Cyber Range Lab Assignment 5

Beyond the Basics of Blockchain & Introduction to Ethical Hacking

Jon Mahoney

SRA 440W

## Beyond the Basics of Blockchain

The first course begins by describing the weaknesses and limitations of blockchain and how these limitations can be addressed. The instructor outlines two solutions, the first being alternate distributed ledger architecture. Some distributed ledger models that were described in the course include linked lists, directed acyclic graphs, and sidechains. These architectures provide solutions to blockchain limitations such as scalability of transaction volume (ex. Bitcoin time limitations), throughput, and lack of support for smart contact technology. The second method to circumvent issues with blockchain is implementing second layer protocols to utilize blockchain while avoiding its weaknesses. An example of a second layer protocol is the Lightning state channel which is used to support transaction speed in Bitcoin. Lightning state channel is used to record the result of a transaction between only two parties. After the transaction occurs, it is recorded and added to the blockchain.

Lastly, the instructor describes advanced ways to provide security within blockchain aside from the standard methods which are public key infrastructure and hash algorithms. The first security method is called multisignatures which describes the process of requiring multiple criteria of verification for a single transaction. For example, an algorithm may check for three out of five secret keys before verifying a transaction. The next method is called zero knowledge proof. A zero-knowledge proof is used to ensure a party knows a secret without revealing the secret. For instance, telling someone the last 4 digits of your social security number proves to them you know the secret (your SSN) without giving them the secret. The last two methods involve ensuring privacy for both parties of a transaction. Each method only provides privacy for one party which is why they are best utilized together. The first method, stealth addresses provide privacy for the recipient of the transaction using a one-time receiving address with an identifier known as a “tag”. This is comparable to a “burner phone” where people make a single phone call and discard the phone as opposed to using a single normal phone for many calls. The security method which supports the sender is called a ring signature. Ring signatures involve signing a message containing a transaction within a group of multiple decoy users.

## Introduction to Ethical Hacking

The second course begins by describing the different types of hackers and the role they play regarding an organization. The types of hackers are ones with malicious intent (black hats), ethical hackers who identify vulnerabilities for the purpose of strengthening security (white hats), and the hacker who exhibits traits of both groups (grey hat). When an organization employs ethical hackers for system penetration testing, they must establish rules and scope for the operation. For instance, an organization may want to test a system in every aspect so they would have no rules and give very little information to testers. By approaching penetration testing in this way, the organization is enabling penetration testers to enter the premise and search trash cans for improperly discarded information or engage in social engineering to phish information out of employees. Another organization may only want to test a specific environment or system so they would impose restrictions on the penetration testers. Additionally, organizations must decide how much information they want to provide to penetration testers. For instance, if you were to hire a penetration tester and provide no information, they will begin searching for vulnerabilities and may find something you missed. The exact opposite is true if you know of a vulnerability and you want data on how it can be exploited. Other noteworthy topics within the course include a lab on the basic commands of Linux which reiterates many of the commands and lessons from our first lab as well as a section on the different hacking tools in Linux.

# Certificates



I don’t know why the hacking certificate says march 8th for completion as it is currently Sunday, March 7th and the Canvas submission will support that.

# Screenshots

             